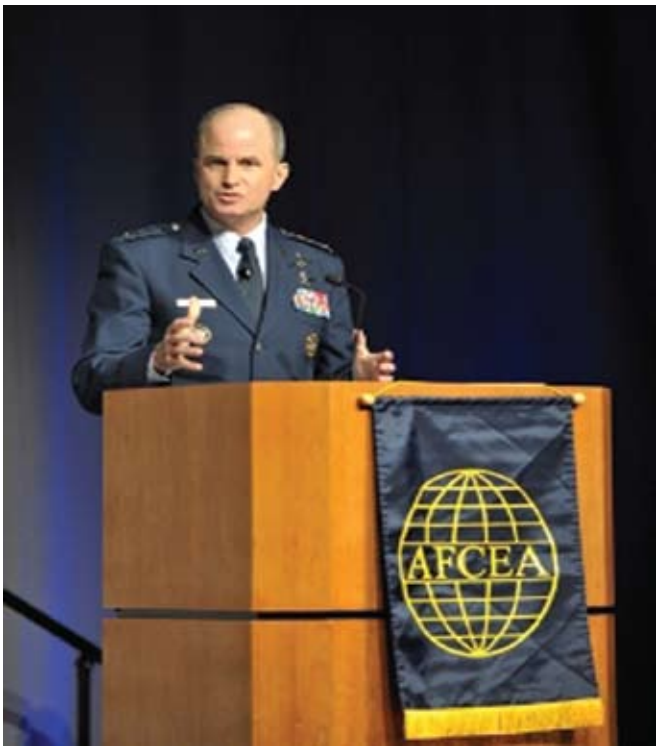
General Kevin P. Chilton on Cyberspace

The Commander of US Strategic Command Opening Remarks at the USSTRATCOM and Armed Forces Electronics Association's 2009 Cyber Symposium

Editor's Note: The inaguaral USSTRATCOM and Armed Forces Electronics Association International (AFCEA) cyberspace symposuim was held in Omaha Nebraska from 7-8 April 2009. Below is the text of General Chilton's Opening Remarks. These remarks are largely unedited.



General Kevin P. Chilton
Source: IO Sphere Staff Photographer

It's great having the Lieutenant Governor here. Mr. Schneider (President and CEO, AFCEA International), what a great partnership with AFCEA. Thank you for being here. I want to recognize Lieutenant General John [Dubia], who's worked so closely with the STRATCOM staff to make this historic first Cyberspace Symposium here in Omaha hosted by US Strategic Command and AFCEA what it is already, which is a resounding success with this outstanding turnout here.

Flag officers from all around the world are here. Military members from every staff of every combatant command, from every service are present here today. We have friends and allies here from around the world that are participating. Great community sponsorship and support from the local community. And of course our industry partners from the great contract community that is so vital to this mission set are also here today, along with our STRATCOM men and women. Thank you all for coming and being a part of this conference today.

These are indeed exciting times at US Strategic Command, and in fact exciting times in US history. Particularly when we start thinking about what's going on in cyberspace.

So what's the origin of this first ever conference here at STRATCOM in Omaha? Quite frankly, it goes back to the videotape [shown] here. When I arrived back in 2007 and we started, focusing on what was most important day in and day out in the command, and those are, as demonstrated in the tape, our three lines of operations.

Of those three, certainly a mission set of deterrence is one that we well understand and have been involved in for many years in this command. Although I would point out it's going to be a new game and it is a new game in the 21st Century, obviously, as compared to the Cold War.

Space, we've been working that line of operation for quite a long time as well.

Certainly the least mature of our lines of operations and arguably one of the most important is the line of operation in cyberspace. When you look at what the President of the United States has asked US Strategic Command to do -- to direct the operations every day of the Global Information Grid that supports our combatant commands and services all around the world every day, to operate it, to defend it, both in peacetime and at war; to be prepared to plan and when directed conduct offensive operations through this medium for this domain; to synchronize operations between combatant commanders in the regions and across the globe; and to be the principal advocate for the capabilities and needs for the warfighters in this domain -- it made perfect sense to bring you all together here in Omaha to help us get our heads around this great mission set that we've been given, this daunting mission set we've been given.

I'll tell you what, we know we don't have all the answers, and often times don't even know what the right questions are to ask. That's why it's so important, if I could echo Mr. Schneider, for you to be a participant in this conference and not just a note taker. I'm going to encourage controversy here. I want to hear both sides of the arguments. And if there are three sides I want to hear the third side as well. I want you to challenge the speakers, challenge the panels, be involved. There's a lot we can learn and there's a lot we must learn.

You've heard in the film, and you've heard Kevin Williams (GISC Director) talk about cyberspace as a domain. That's the way I think about it. In fact I try to break things down pretty simply for myself, just so I can get my head around it. We have the air domain, we have the land domain, we have the maritime domain, we have the space domain, and we have the cyberspace domain. The first three can be pretty much defined by geography

or range of operation. The last two are absolutely global in nature. In fact they are agnostic to the artificial lines that we may draw on a map. They can care less about the location of continents and oceans. Space and cyberspace are cross-cutting domains, but they're every bit as much like air, land and sea -- warfighting domains, domains that we can expect to be challenged in, domains that we need to and depend on to conduct full military operations as well as commerce that supports the economy. They demand freedom of action, each one of those domains, and so does cyberspace.

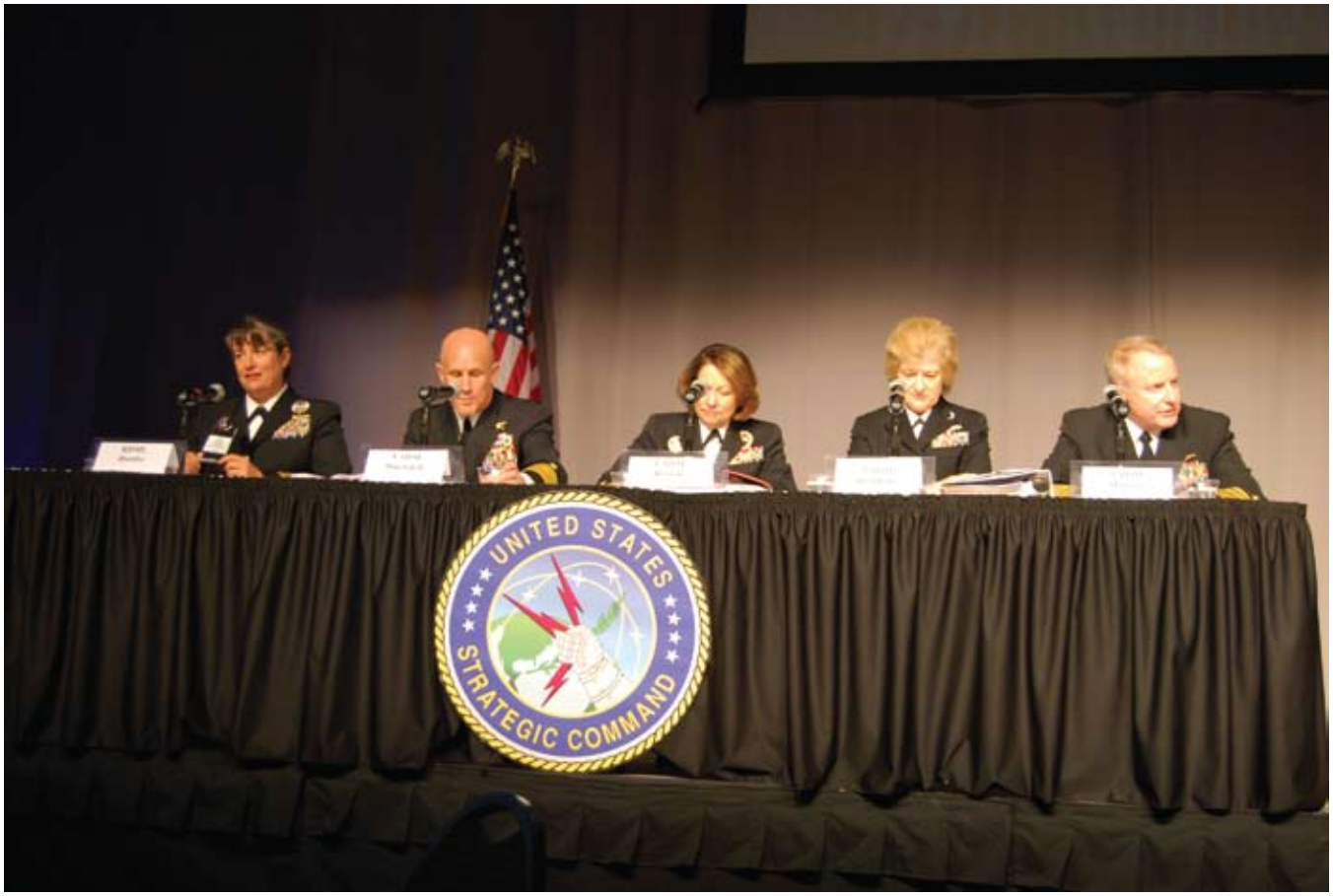
For the seas, the maritime domain, demands freedom of action for commerce and in wartime for logistic resupply and movement of troops and ammunition and equipment forward to far-off theaters.

The global cyberspace domain is how we move information. It's how we move orders. It's how we move thought. We need that to be secure and available to us to freely operate in, both in peacetime and at war.

I'd like to give a little perspective on where I feel like we are in this great venture of taking on the mission set in cyberspace. I'm going to flash back, use my time in the military and set it back in the same period of time or the same length of time back in history.

I've been in the Air Force, commissioned for 33 years now, so I'm going to take us back to 1893 and I'm going to commission 2nd Lieutenant Chilton, graduating from the US Military Academy at West Point where I probably spent a lot of time studying land warfare. I probably spent a lot of time studying lessons learned from the Civil War and increased firepower and the power of defensive positions versus frontal assault. I probably learned a few things about what happened to Custer in 1876 and operations in the west. I probably didn't think or was not educated one iota about the thoughts of how one might use a new domain for warfare called air beyond maybe balloons for artillery spotting.

1893. Why did I pick that year? Because 10 years later, in 1903, the Wright Brothers flew. Suddenly there was a new domain available. It was nascent, but it was there. And 33 years later, after being commissioned 2nd Lieutenant Chilton found himself in 1926. And not only had they had added manned flight to that thought in that domain in World War I, he was thinking about how he was going to fight the next fight in that domain and how important it was to protect that domain, and the growing importance of that domain to commerce and freedom and transportation and the development of this country.



Senior Leader Panel Discussion at the Cyberspace Symposium
Source: IO Sphere Staff Photographer

Cyber Symposium Vendor and Organization Display Area
Source: IO Sphere Staff Photographer

In 1976 when I entered the Air Force as a commissioned Air Force officer I was one year past having turned in my slide rule and buying my first HP-35 handheld calculator for $275. [Laughter]. The concept of a laptop or a desktop computer was not taught at the Air Force Academy when I was there. Yet 10 years later, in 1986, when I arrived at NASA someone came in and put this thing on my credenza, moved my files out of the way and moved some books out of the way and set this screen on my credenza and a keyboard and shoved something under my desk and said here is your computer. It was a Wright Brothers moment, if you will, in cyberspace for me. [Laughter].

Now, 33 years later, in 2009, I am dependent on cyberspace. I'm dependent on it in my personal life. This country's dependent on it for commerce and its economy. And warfighters around the world are dependent on it to conduct operations not just in cyberspace, but in every other domain. Thirty-three years this happened. Faster than the revolution of flight.

Just think about it. In 1981 there was this really bright young man named Bill Gates who said you know, I think 640K of memory is about enough for anybody to use. I can't imagine ever needing more than that. Bill Gates, 1981. Talk about change.

In 1991, I remember in NASA we upgraded the space shuttle main computer. We doubled its computing capacity from 128K to 256K. [Laughter]. That's the computer we still use today to go to and from orbit in the space shuttle -- 256K. The pace of change in this domain has been absolutely outstanding.

If I could continue on with the airplane metaphor and take us back to World War I, I think there may be some analogies there as well. In the early days of World War I the German aviators would be up and the French aviators would be up on the other side of the line, and really they were kind of looked at as non-combatants. Mostly what they were doing was observing or spying, collecting information from that domain. They were even known on occasion to pass close enough to see each other in cockpits and wave to each other as they went by -- a rather gentlemanly approach to this new domain. We were enemies, they said, but we should not forget the civilities.

Now there's a legend told about one fateful day when a German and French pilot passed each other, and the German pilot must have had a bad morning because he shook his fist at the French pilot as he went by, as the Frenchman said in a rather blustery and caddish way. Well, the next day when the German approached he hurled some sort of missile at the French pilot as he rode by, and the French pilot was so incensed that he dove at the enemy, and I love this part, drew a small flask of port wine from his pocket -- [Laughter] -- and bounced it off the exhaust manifold of his boorish antagonist. I love it. Flying with a bottle of wine. [Laughter].

As the legend goes, that marked the end of courtesy in the air domain and the beginning of hostilities. What followed, though, was a dramatic change in three areas, in my view. There was a change in culture, in the warfighting culture, and how we thought about using this new domain. There was a change in conduct, in rules of engagement, on how we valued and treated this new domain of air. And there was a dramatic and measurable change in the capabilities and the treasure we would invest to develop those capabilities in this domain.

We have moved past the civilities in the cyber domain. US forces and those of our adversaries now rely heavily on their computer networks for command and control, for intelligence, for planning, for communications, for conducting operations. But these architectures are vulnerable. In fact for more than 15 years the US government and DoD networks have come under increasing pressure to attacks and probes from adversaries, as diverse as nation states, to the disgruntled individual or bored teenage hacker. And while we have detected illicit activity on our networks for more than 15 years and employ resources to offer a comprehensive multi-disciplinary approach to protecting our networks, we need to do more.

All of us, all of us -- me included -- are making it too easy for our adversaries to exploit our networks today. Like the World War I aviators we need a change in our culture, our conduct, and in our capabilities if we're going to advance the state of art and provide the protection and freedom of action we need in this domain. Let me begin first with culture.

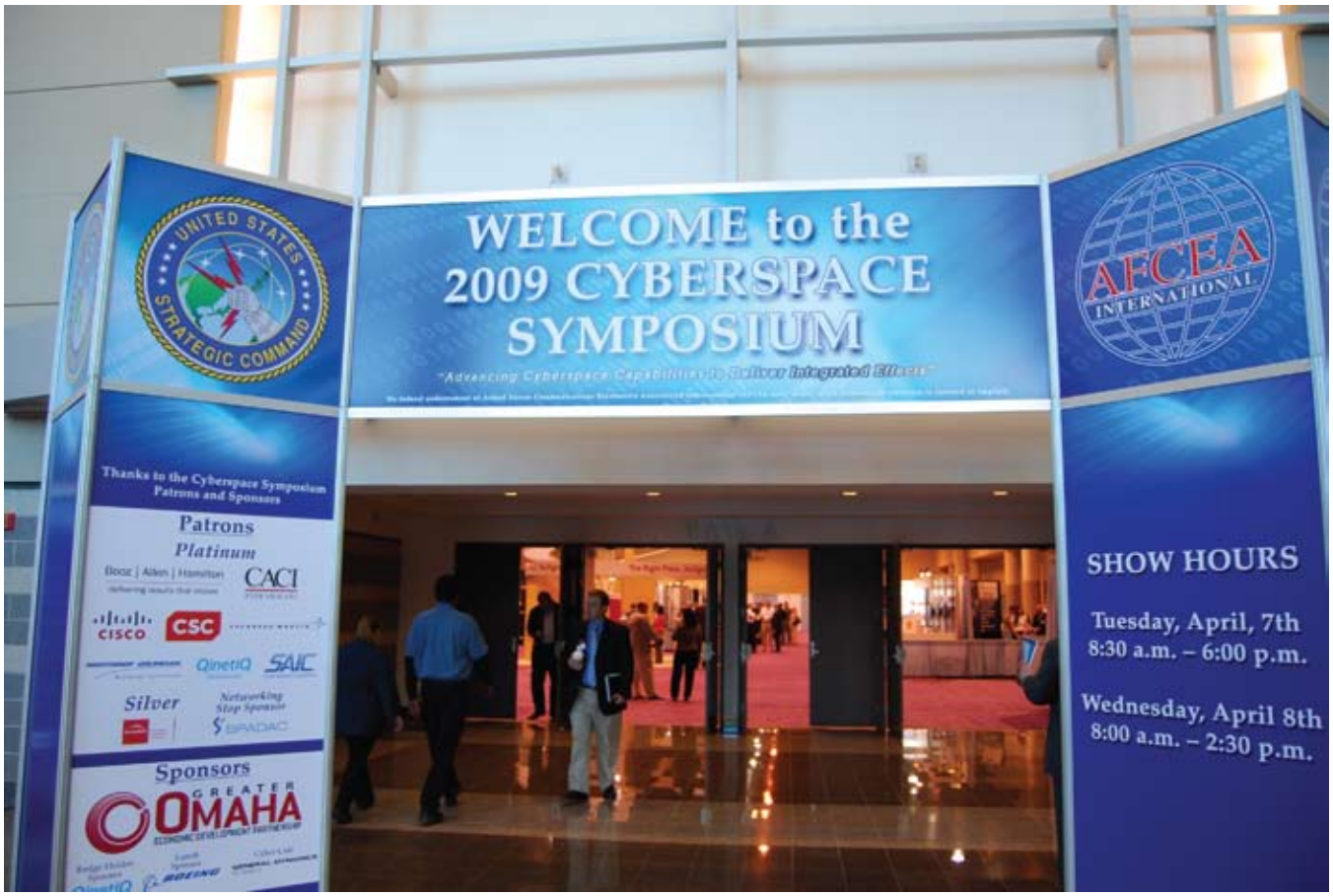
Cyberspace really grew up as a confluence of technologies that evolved in today's globally connected networks. In fact I reflected on my experience at NASA, I remember after they put that computer on my desk I successfully ignored it for about a month. I'd have to dust it on occasion and I would gripe about it being in the way of my in-box on occasion, but inevitably one day I missed a meeting. I asked the person who had organized the meeting, I said why didn't you tell me the meeting was happening? They said well, I sent you an electronic message. I said why didn't you just call me? Why didn't you just holler at me? We shared a desk in the same office. This person had moved on and I had not begun the cultural shift into cyberspace. And in fact what happened then, in my view, is the culture that we developed because of the way it grew was one of cyberspace as a convenience. It wasn't convenient for this person to call me, and they couldn't be interrupted long enough or thought I was too busy to be interrupted as I worked at my desk so they sent me an electronic message. We didn't call them e-mails in those days.

Think about it. When there was a problem with your computer, who did you call? The smart young technician, the information assurance person that works in your office. Or do you call the J6 or the A6, N6, G6, and say get down here and fix my darn computer -- it's not working. And they did. And they do. And they come and fix those machines. And we developed this culture, in my view, that the cyber domain, the computers on our desks are there just for convenience. They are not part of a warfighting domain. But in fact, they are. And they are not just J6 problems. It is commanders' business.

And this is a cultural shift that we must make. We must think about this domain and the tools in this domain and the readiness of this domain as commanders, as essential to successful operations.

When I was a wing commander of the U-2 (Beale AFB, CA) I reviewed the maintenance statistics on my airplanes every day. Why? Because I couldn't fly them if they weren't maintained properly and if they weren't prepared to operate. We need to review the maintenance statistics and the readiness of our cyber networks -- we're commanders and we depend on them -- and I challenge anyone to claim they're not -- every day. That's a mindset change.

It's not a convenience any more, it's a dependency. We need to recognize that we need this domain and we need these systems to conduct our fight today and tomorrow. We need to recognize that we



US STRATCOM and AFCEA Cyberspace Symposium Entrance
Source: IO Sphere Staff Photographer

can fight in this domain just as an air-to-air fighter can fight in the air domain; and we can fight through this domain and affect other domains just as an airplane can drop a bomb on a land domain and create affects across a domain. And as commanders we must appreciate the vulnerability of this domain, not just its importance. We have to transition from a culture of convenience to a culture of responsibility. We must recognize vulnerability -- the vulnerability that one system can create here on the other side of the world, not just locally.

Every Soldier, Sailor, Airman, Marine in the military is on the front line of cyber warfare every day. If you think about the guards who guard your bases, who stand there at the gate and make sure only the right people come in and keep the wrong people out -- that's everybody who has a computer on their desk in these domains today. They are part of the front line of defense and in fact they're engaged in cyber operations that matter every day, whether they know it or not.

Changing this culture is absolutely important and it's going to take, I believe, the longest period of time.

Conduct. How do we conduct ourselves?

If you look at every other domain and every other system, one of the first principles, one of the first things we focus on is our people and their training. Correct? Land warfare, sea warfare, air warfare, special operations. We think about the training of our people because we know, tools aside, that's our leverage point in any conflict.

I'm required to train on cyberspace security by my service, by my command, every year. I get a little thing that blinks up on my computer that says you are due for information assurance training, General Chilton. Get it done by this date. Once a year. Once a year! And I get to read and study year-old adversary tactics, techniques and procedures against an adversary who's changing those every day. Perhaps every hour.

We're not training right. We need to adjust that.

Inspections. As the commander of an aircraft wing I expect my higher headquarters to come down and give me an annual operational readiness inspection to make sure I can do the mission I've been given. So what did I pay attention to in the way of that machine? I paid attention to maintenance, logistics, the readiness of my air crews, their ability to fly the mission and do the job and get back.

What didn't I pay attention to? The cyberspace tools that I needed to get them off the ground. Where are all the tech orders now that our people use to maintain our airplanes? Are they on paper any more? Are they on classified networks? No, they're on unclassified networks and they're on laptop computers or handheld devices that are vulnerable. Change the tech orders on your maintenance manuals on the flight line and watch what happens.

Is cyberspace essential to operations today? Should we be inspecting the readiness of every organization that relies on cyberspace to conduct their operations? Should commanders care about that? Should they be graded about that? I believe they should.

Cyberspace Symposium Conference Room
Source: IO Sphere Staff Photographer

When an airplane crashes, when a ship runs aground, if a tank goes off the road and rolls inverted in a ditch, what's one of the very first thing commanders do? They stand up an investigation board, a mishap board, because they want to get to the root cause, they want to fix the root cause. They study that, they take lessons learned, they promulgate it through training, and they make sure the force learns from those mistakes or learns from those tragedies. Then they also go down and find out why it happened and if there was any culpability involved in that.

Do we do that today in cyberspace? Do we have the tools to hold people accountable for not following rules and regulations? We do. We do. It's called the UCMJ. We've got all the authority we need to do that, but we can't get this backwards. We can't hold people accountable if we haven't properly trained and equipped them. We need to do that. Properly train, properly equip, properly educate, conduct mishap investigations when they happen, and then hold people ultimately accountable for their behavior.

There are lots of violations that occur today in cyberspace and on our military networks. It happens today. People think the rules don't apply to them, for whatever reason. Operational necessity is viewed in their minds, laziness, whatever. But I'll tell you what, when we do that there are adversaries out there who are today taking advantage of that misbehavior and that lack of discipline.

Another point on conduct. When we think about how we're going to conduct operations and ensure the defense of the network. This is anathema to many many folks. It's the concept of centralized command and decentralized control. It's absolutely necessary in my view in this global domain that requires people to be compliant, requires hardware to be upgraded quickly, and requires defensive systems that are going to operate and work properly.

When I asked last year how many SIPRNET and NIPRNET machines were on the DoD network it took over 45 days to get the answer. I'm not sure I got the right answer after 45 days, ladies and gentlemen.

Now if I asked General Casey how many M-16s there were in the Army he could tell me, I'll bet, within 48 hours. I know Chief Schwartz could tell you how many M-9s there are in the Air Force because every one of them is signed in and signed out; there's 100 percent accountability for those weapons, that if we lose control of might be used to hurt somebody within the ballistic range of that weapon. And yet we have computers out there that we don't know the configuration of, we don't know the location of, we don't know who's on them, who if misused can affect operations on the other side of the world, not just in the room you're sitting in. Culture change, conduct change, and the way we address this.

I shouldn't have to ask how many computers are out there. We should know and we have the technology today. We need to deploy it so that we know every day what's on our network, what's plugged in, what its configuration is. Does it have the latest anti-virus injected in it and updated in it? Have the latest orders gone out? How's our training? Et cetera. That should be machine to machine and it should be automated. We can do it. We need to get on with it.

Changes to culture, conduct, capabilities. Our people need better tools out there today, particularly at the command and control level, at the operational level of war, at JTF GNO, at JFCCNW, our operational component commanders who operate, defend and do the missions in this domain. They need the tools that allow them to better manage the operation of and the defense of this network at network speeds. As long as we're depending on the human element, which we can never forget, but as long as that's our principal dependence is on the human element and we operate at human speeds we will be outside the turning circle of our adversary.

We need to operate at machine to machine speeds. We need to operate as near to real time as we can in this domain. We need to be able to push software upgrades automatically. AOL does that on my home computer, why can't we? We need to have our computers scanned remotely with the last anti-virus software. We need the host base security system deployed this year, not five years from now when we can afford it, because we can ill afford not to have these technologies available for us today.

We need common operating pictures, just like commanders in every other domain demand. Today if you look at our common operating picture in cyberspace, as General Pollett's command and control center, you will find places in the United States of America that are black holes. Black holes. Why? Because we don't know what's going on there. And you know what's around those black holes typically? The fences of one of our military installations, because we have put up artificial barriers to keep the centralized command and control authority -- the mission assigned by the President to operate and defend, outside our perimeter. They say it's "my network." No, it's not. And a vulnerability in "your network" is a vulnerability to the entire GIG.

This concept of centralized command and control, decentralized execution I believe is absolutely necessary for our operations in this command.

But you know, at the end of the day I believe we ultimately have to be even faster than network speed if we're going to defend this network appropriately. How do you do that? I'm not defying the laws of physics here. You do it by focused high-tech intelligence. You do it by focused high-tech intelligence, focused all-source intelligence, that tries to get you out and anticipate threats before they arrive. You have to be able to anticipate them and when you can preempt those threats and preempt those attacks before they arrive at your base, post, camp or station, or at your laptop on your desk.

Finally, what we need in the capabilities area is more people. More people dedicated and focused in this mission area. The services are great at organizing,

training and equipping air, land, sea and space domain forces. We need to move forward in organizing, training and equipping cyber forces to conduct these critical operations for the Department of Defense.

Ladies and gentlemen, today as you heard the Lieutenant Governor say, leaders in government, business and academia have moved from ruminating about threats in cyberspace to treating them as real and present dangers. We know we must make this transition. We have seen government networks probed in the past, and I firmly believe these intrusions will only continue to increase as we move forward.

The cost has been in the hundreds of millions of dollars. We do a poor job of quantifying it, but they are real dollars and real costs. The cost has been in lost and exploited information that can be used against us in future conflicts to interdict our operations, to inhibit our operations, or put us in a position to be less effective in the other domains as well as in cyberspace.

Our challenge will be to prevent attacks on our networks and cross-domain servers by coming through our networks. Our challenge will be to find ways to interdict attacks when they've been launched. And when they are successful our challenge will be to make the adversary stop the attack.

I think the most difficult challenge that we have today will be the challenge of continuing to operate our networks when we come under attack.

Think about any other domain. I think about my training in the Air Force. When we went to Condition 4 at the base incoming ballistic missiles with chem/bio gear, chem/bio attack potential. Yeah, we got it for the initial explosion, but then we went out into that hostile environment with our MOPP gear on and we fixed airplanes and we loaded airplanes and we got in airplanes, we took off and flew, we conducted operations in a hostile environment. That's what cyberspace is going to be, and the hardest thing is going to be to fight through attacks in the future and ensure that the domain continues to operate in at least an adequate fashion so we can continue operations in every other warfighting domain.

Ladies and gentlemen, this conference I believe provides a unique opportunity for all of us to get at the latest cutting edge ideas from a cross section of cyberspace stakeholders. From the technologists to the warfighters to the operators to the intelligence community to the wire pullers to folks in other domains who don't think much about cyber day in and day out but understand and know in the back of their minds they are dependent on this domain. You all are here today and we have a great opportunity as we move forward for the next couple of days to share ideas and challenge paradigms and look for the problems we need to solve and the potential solutions to solve them as we move forward.

Folks, I want to really particularly thank Mr. Kevin Williams and his [GISC] staff for the great work that they have done in putting this conference together and giving us this opportunity to get together; AFCEA for all the great partnership we have with you; for government, industry and academia partners who are here today, who have taken so much time from their busy schedules, to get us ready and go forward.

We've got an all star lineup of speakers and panelists that are going to entertain you, but hopefully more importantly challenge you, and I look forward to hearing your thoughts and questions over the next couple of days.

We must leave no stone unturned. The mission we have today in the US Strategic Command is focused on DoD networks. But let's not fool ourselves. The threat to America goes beyond that. The threat to cyberspace entities in America that can affect our economy, our industrial base, our power and telecommunications, our banking, our finance systems, the threat is real today. We need to be thinking about how that is going to be protected in the future.

Remember, all of our DoD networks run on the same wires so there's synergy there in thought when we think about how we're going to move forward in both the DoD and the broader Department of Homeland Security effort to secure America against pending threats.

Finally, I particularly want to challenge everybody that's come from out of state, from around the country and indeed around the world, to take home what you've learned, what you will learn here in the next few days; to challenge people back home; share the information, share your ideas. But without you today going home and spreading the word we cannot begin to change our cyber culture, our cyber conduct or our cyber capabilities.

Thanks, ladies and gentlemen. It's great to be with you here this morning.

General Kevin P. Chilton is Commander, United States Strategic Command, Offutt Air Force Base, Nebraska. He is responsible for the global command and control of U.S. strategic forces to meet decisive national security objectives. USSTRATCOM provides a broad range of strategic capabilities and options for the President and Secretary of Defense.